

REMARKS

The Examiner indicated that drawing corrections were needed, and specifically to include the access server recited in the claims and described in the specification. Such have now been included in the drawings of Figs. 1A, 1B and 1C in the replacement sheets.

Corresponding description changes have been made to paragraphs [0025], [0026] and [0027] to include reference to the access server. Also, it was noted that no specific reference in the specification was made to the service provider network originally shown in these drawings and accordingly such has also been added to these paragraphs.

No new matter has been added either in the specification or in the drawings.

The Examiner had rejected claims 1, 3, 5-7, 11-13, 15-18, 26-29 and 31-33 under 35 USC 102 (a) as being anticipated by U.S. Patent Application Publication No. 2003/0140151 to Daenen et al. (hereinafter Daenen) and the remaining claims under 35 USC 103(a) as being unpatentable over Daenen and further in view of U.S. Patent 7,073,055 to Freed et al. (hereinafter Freed).

Applicants specifically wish to point out that the Service Policy Director as recited and claimed is a device separate and apart from any access server or authentication server. This was clarified in the previous amendment. However, the claims also point out that what this Service Policy Director does is extract information from the authentication message which is acted upon by the access server and the authentication server. The Service Policy Director after extracting the information from the authentication message then goes on to make use of that information to set up a user policy table. However, the claims point out that the user policy table that is then set up in a separate piece of equipment namely, the Service Policy Director, is then used to manage subsequent user traffic which takes place after the authentication message occurs. The claims are clear and have even been further clarified to point out that this user policy table which is set

up on the Service Policy Director is utilized during ongoing traffic that occurs after the authentication takes place.

While the Examiner has referred to specific locations in Daenen pointing that the CPRS can be a separate piece of equipment, at no place in Daenen does it indicate that the CPRS does anything but participate in the authentication process. That is all the CPRS does. Daenen discusses whether the CPRS is a part of the BAS or a separate piece of equipment. However, whether it is a separate piece of equipment from the BAS or a part of the BAS it only participates in the authentication process. There is absolutely nothing in Daenen that hints or suggests that the CPRS would be used subsequent to the authentication process. Quite the contrary, Daenen specifically indicates that it would not be used in subsequent user traffic.

In that regard, the Examiner has referred to paragraphs 32 and paragraph 51 of Daenen to indicate the use of the CPRS. In looking at paragraphs 32 and 51, all it indicates is that the CPRS can be a separate piece of equipment from the BAS. However, the function of the CPRS is described at the end of paragraph 62. It there states as follows:

“The CPRS is used during the connection setup. Once the IP layer is established between the end-user and the VPN, the data stream goes via the BAS directly to the VPN, without passing via the (sic) CPRS (routing).” (Emphasis added)

This clearly points out that the CPRS takes no part in the subsequent user traffic. This is further confirmed in paragraph 15. There it states that once the user has been connected to the VPN zero, the CPRS can relate the “other requests” from the same user to each other. This is further clarified in paragraph 15 by stating that this relation can be used by the provider for

applying policies on “these” further “access requests” or for monitoring these access requests in the related context.

Accordingly, it is clear that the CPRS is only used in connection with access requests or further access requests. However, beyond the access request, once access has been attained and authorization has been completed, as it clearly states in paragraph 62, it does not take part at all in any further user traffic.

Accordingly, any type of policy that is set up in Daenen only is for use during the actual authorization process. Daenen does not provide any teaching, suggestion, or in any connection whatsoever anything related to subsequent user traffic.

In that regard, the Examiner should also view Freed in the same context. The Examiner recognized that Freed was not subsequent user traffic. The Examiner looked at the various policy setups in Freed and tried to apply it to applicant’s Service Policy Director. However, neither Freed nor Daenen teach about subsequent user traffic after authorization. Both Freed and Daenen are only talking about authorization processes using pieces of equipment only to deal with the authorization server. Once authorization takes place, neither of these teach anything concerning the ongoing process.

Applicant, on the other hand, provides a unique piece of equipment. Not only does it provide policy during subsequent traffic after authorization, but applicant teaches a piece of equipment which extracts information from the authorization process and based upon the information that it extracts during the authorization process it then sets up a policy for ongoing communication subsequent to the authorization process.

Nothing in either of the references in any way suggests extracting information from the authorization process to set up a separate policy which would be utilized during subsequent traffic after the authorization process is completed.

Although it is believed the original claims already brought out the above-mentioned distinction, in order to further highlight this feature, the claims have been further amended to specify that the subsequent user traffic is traffic directed to a service providing server and clarifying that all of this traffic is after the access server and authentication server go through the authentication process.


It should further be noted that some of these policy descriptions that the Service Policy Director extract from the authentication message and apply during subsequent user traffic after the authentication process, are especially innovative as for example the ability to pass traffic through a security gateway before sending it to the requested server based on such policy, and the ability to redirect user traffic to a different server than the one the user requested (like a cache server) based on the policy. It should be noted again, that these policy decisions are extracted from the authentication messages and then are used by this separate piece of equipment during processing after the authentication message, namely during subsequent traffic.

It is believed that none of the references taken alone or in combination teach this concept. Accordingly, it is believed that the present claimed invention is patentable over the cited

references. Should the Examiner have any questions with respect to this Amendment it is kindly requested that the Examiner contact Applicant's attorney at the number listed below to see if this application allowance can be expedited.

Any fee due with this paper may be charged on Deposit Account No. 50-1290.

Respectfully submitted,

/Samson Helfgott/ 
Samson Helfgott
Reg. No. 23,072

CUSTOMER NUMBER 026304

PHONE: (212) 940-8800

FAX: (212) 940-8986

Docket No.: 101092-00072 (RADW 20.114)

SH:tb